Vereinbarung zur Auftragsverarbeitung nach Art. 28 DSGVO

Stand: 02.10.2026

zwischen dem Kunden von mein-angestellter.de, der als Unternehmer handelt, als Verantwortlichem (im Folgenden „Kunde“) und der A-Z Geschäftsbesorgungs UG (haftungsbeschränkt), Wilhelm-von-Siemens-Straße 16–18, 12277 Berlin, als Auftragsverarbeiter (im Folgenden „Anbieter“).

Diese Vereinbarung wird bei der Registrierung abgeschlossen und gilt für die gesamte Dauer des Nutzungsvertrags über mein-angestellter.de. Sie geht den Allgemeinen Geschäftsbedingungen in Fragen des Datenschutzes vor.

§ 1 Gegenstand und Dauer

1. Der Anbieter verarbeitet personenbezogene Daten im Auftrag des Kunden, soweit der Kunde die Plattform mein-angestellter.de und den digitalen Mitarbeiter Okto nutzt, insbesondere für E-Mail, Abläufe, Ablage, Kunden und Objekte, Rechnungswesen, Kalender, Teamverwaltung und die Bearbeitung von Aufträgen durch Okto.
2. Die Verarbeitung dauert so lange wie der Nutzungsvertrag und endet mit der Löschung oder Rückgabe der Daten nach § 9.
3. Daten, die der Anbieter für eigene Zwecke verarbeitet, etwa Konto-, Abrechnungs- und Rechnungsdaten des Kunden, sind nicht Gegenstand dieser Vereinbarung. Dafür gilt die Datenschutzerklärung.

§ 2 Art und Zweck der Verarbeitung, Datenarten und betroffene Personen

1. Art der Verarbeitung: Erheben, Speichern, Ordnen, Abfragen, Verwenden, Übermitteln an die in Anlage 2 genannten Unterauftragsverarbeiter, Offenlegen gegenüber Empfängern, die der Kunde über geteilte Links bestimmt, Einschränken und Löschen.
2. Zweck: Bereitstellung der Plattform und Bearbeitung der Aufträge des Kunden nach dessen Weisungen.
3. Datenarten: Kontakt- und Stammdaten, Kommunikationsinhalte, Inhalte von Dokumenten und Dateien, Kunden-, Objekt-, Ablauf- und Belegdaten, Termin- und Aufgabendaten sowie Nutzungs- und Protokolldaten, einschließlich der Zugriffsprotokolle geteilter Links (Zeitpunkt, Aktion, Datei oder Ordner, Name und E-Mail-Adresse oder Konto des Empfängers, gekürzte IP-

Adresse, grobe Browser- und Betriebssystemangabe), soweit der Kunde sie in die Plattform einbringt oder über Integrationen freigibt.

4. Betroffene Personen: Beschäftigte des Kunden, Kunden und Interessenten des Kunden, Lieferanten, Geschäftspartner, Empfänger geteilter Links und sonstige Kontaktpersonen des Kunden.
5. Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO verarbeitet der Anbieter nur, wenn der Kunde sie in einem dafür ausdrücklich vereinbarten Verarbeitungsmodus einbringt.

§ 3 Weisungen

1. Der Anbieter verarbeitet die Daten nur auf dokumentierte Weisung des Kunden, es sei denn, er ist nach Unionsrecht oder dem Recht eines Mitgliedstaats zur Verarbeitung verpflichtet; in diesem Fall teilt er dem Kunden diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das Recht dies nicht verbietet.
2. Weisungen sind diese Vereinbarung, die Nutzung der Funktionen und Einstellungen der Plattform – einschließlich des Erstellens, Änderns und Beendens geteilter Links – sowie Aufträge an Okto. Weitere Weisungen erteilt der Kunde in Textform an datenschutz@mein-angestellter.de.
3. Ist der Anbieter der Ansicht, dass eine Weisung gegen Datenschutzvorschriften verstößt, informiert er den Kunden unverzüglich und darf die Ausführung bis zur Bestätigung oder Änderung aussetzen.
4. Der Kunde teilt Inhalte nur mit Empfängern, gegenüber denen er zur Offenlegung berechtigt ist, und informiert sie, soweit erforderlich, über die Verarbeitung.

§ 4 Vertraulichkeit

Der Anbieter stellt sicher, dass die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Betreiberpersonal liest keine Geschäftspost und keine Inhalte des Kunden, soweit dies nicht zur Erfüllung eines Auftrags, zur Behebung einer Störung oder aufgrund gesetzlicher Pflichten erforderlich ist.

§ 5 Technische und organisatorische Maßnahmen

1. Der Anbieter trifft die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen. Sie sind in Anlage 1 beschrieben.
2. Die Maßnahmen dürfen weiterentwickelt werden, sofern das Schutzniveau nicht unterschritten wird.

§ 6 Unterauftragsverarbeiter

1. Der Kunde erteilt die allgemeine Genehmigung, Unterauftragsverarbeiter einzusetzen. Die bei Vertragsschluss eingesetzten Unterauftragsverarbeiter sind in Anlage 2 aufgeführt und gelten als genehmigt.
2. Der Anbieter informiert den Kunden mindestens 14 Tage vor dem Einsatz eines neuen oder dem Austausch eines Unterauftragsverarbeiters in Textform oder in der Plattform. Der Kunde kann aus wichtigem datenschutzrechtlichem Grund innerhalb dieser Frist widersprechen. Kann der Anbieter den Einwand nicht ausräumen, kann der Kunde den Nutzungsvertrag außerordentlich kündigen.
3. Der Anbieter verpflichtet Unterauftragsverarbeiter vertraglich auf Datenschutzpflichten, die denen dieser Vereinbarung im Wesentlichen entsprechen. Übermittlungen in Drittländer erfolgen nur unter den Voraussetzungen der Art. 44 ff. DSGVO, insbesondere auf Grundlage des Angemessenheitsbeschlusses zum EU-U.S. Data Privacy Framework oder der Standardvertragsklauseln der Europäischen Kommission.

§ 7 Unterstützung des Kunden

1. Der Anbieter unterstützt den Kunden mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von Anträgen betroffener Personen, insbesondere durch Funktionen zu Auskunft, Export und Löschung in der Plattform. Wendet sich eine betroffene Person direkt an den Anbieter, leitet er das Anliegen an den Kunden weiter.
2. Der Anbieter unterstützt den Kunden unter Berücksichtigung der ihm vorliegenden Informationen bei den Pflichten nach Art. 32 bis 36 DSGVO.

§ 8 Meldung von Verletzungen

Der Anbieter meldet dem Kunden eine Verletzung des Schutzes personenbezogener Daten unverzüglich, nachdem sie ihm bekannt geworden ist. Die Meldung enthält, soweit bekannt, die Informationen nach Art. 33 Abs. 3 DSGVO. Der Anbieter ergreift unverzüglich Maßnahmen, um die Verletzung einzudämmen und ihre Folgen zu mildern.

§ 9 Löschung und Rückgabe

1. Während der Laufzeit kann der Kunde Daten über die Funktionen der Plattform exportieren und löschen.
2. Nach Vertragsende löscht der Anbieter die im Auftrag verarbeiteten Daten, nachdem der Kunde Gelegenheit zum Export hatte, spätestens 90 Tage nach Vertragsende, sofern keine gesetzliche Pflicht zur Speicherung besteht. Daten in Sicherungskopien werden mit dem regulären Überschreiben dieser Sicherungen gelöscht und bis dahin nicht mehr verwendet.

3. Auf Wunsch bestätigt der Anbieter die Löschung in Textform.

§ 10 Nachweise und Überprüfungen

1. Der Anbieter stellt dem Kunden die zum Nachweis der Einhaltung dieser Vereinbarung erforderlichen Informationen zur Verfügung.
2. Überprüfungen, einschließlich Inspektionen, durch den Kunden oder einen von ihm beauftragten, zur Verschwiegenheit verpflichteten Prüfer sind nach angemessener Vorankündigung zu den üblichen Geschäftszeiten möglich, grundsätzlich höchstens einmal im Kalenderjahr, es sei denn, ein konkreter Anlass rechtfertigt eine weitere Prüfung. Die Rechte der Aufsichtsbehörden bleiben unberührt.

§ 11 Haftung und Schlussbestimmungen

1. Für die Haftung gilt Art. 82 DSGVO.
2. Änderungen dieser Vereinbarung bedürfen der Textform. Bei Widersprüchen geht diese Vereinbarung den AGB vor.
3. Es gilt deutsches Recht.

Anlage 1 – Technische und organisatorische Maßnahmen

- Zutritt: Die Systeme laufen in Rechenzentren der in Anlage 2 genannten Hosting-Anbieter; deren physische Sicherung liegt bei diesen Anbietern.
- Zugang: Anmeldung nur mit persönlichem Konto und Passwort von mindestens zehn Zeichen; Passwörter werden ausschließlich als Hash gespeichert. Neue Konten bestätigen ihre E-Mail-Adresse. Deaktivierte Nutzer verlieren sofort alle Sitzungen und Zugangsschlüssel. Geteilte Links verwenden zufällige, nicht erratbare Schlüssel; sie werden als Prüfwert und – damit die erstellende Person und die Inhaber des Kundenkontos sie erneut abrufen können – verschlüsselt gespeichert. Links haben ein Ablaufdatum von höchstens einem Jahr, können ein Passwort mit Sperre nach wiederholten Fehlversuchen verlangen und sind jederzeit widerrufbar. Links deaktivierter Nutzer sind sofort unwirksam. Links nur für Konten verlangen ein Konto mit bestätigter E-Mail-Adresse.
- Zugriff: Rollen und Berechtigungen je Kundenkonto (Inhaber, Büro, Objektleitung); Betreiberpersonal hat keinen Zugriff auf die Geschäftspost des Kunden und kann Belege des Kunden weder anlegen noch festschreiben. Über einen Link sind nur Inhalte erreichbar, die die erstellende Person selbst sehen darf; private Ordner anderer Personen sind ausgeschlossen. Betreiberpersonal kann keine Links erstellen; Links, die ein Konto verlangen, öffnet es nur, wenn der Kunde das Konto der betreffenden Person ausdrücklich einträgt.

- Trennung: Jeder Datensatz ist genau einem Kundenkonto zugeordnet; Abfragen werden serverseitig auf das angemeldete Kundenkonto beschränkt. Inhalte geteilter Links stammen ausschließlich aus dem Kundenkonto, in dem der Link erstellt wurde.
- Weitergabe: Übertragung ausschließlich verschlüsselt über HTTPS/TLS. Vor jeder KI-Anfrage werden in der Standardeinstellung E-Mail-Adressen, Telefonnummern, IBANs und Anschriften durch Platzhalter und bekannte Kontaktnamen durch interne Kundennummern ersetzt.
- Eingabekontrolle: Sicherheits-, Abrechnungs- und Berechtigungsvorgänge werden mit Zeitpunkt und handelnder Person protokolliert. Außenaktionen von Okto, etwa Versand oder Festschreibung, erfordern eine ausdrückliche Freigabe. Erstellen, Ändern und Beenden geteilter Links sowie Zugriffe über geteilte Links werden protokolliert; Zugriffsprotokolle werden nach 180 Tagen gelöscht. Zugriffe von Teammitgliedern sehen namentlich nur die Inhaber des Kundenkontos. Okto legt keine Inhalte in Ordner, die über Links nach außen geteilt sind.
- Verfügbarkeit: Datensicherungen beim Hosting-Anbieter; Begrenzung von Anfragen gegen Überlastung und Missbrauch.
- Organisation: Verpflichtung der befugten Personen auf Vertraulichkeit; Löschprozess nach § 9 und nach Art. 12 und 17 DSGVO. Gelöschte Dateien werden nach 30 Tagen im Papierkorb endgültig gelöscht.

Anlage 2 – Unterauftragsverarbeiter

- ALL-INKL.COM – Neue Medien Münnich, Hauptstraße 68, 02742 Friedersdorf, Deutschland: Hosting von Website, Plattform, Datenbank, Ablage und E-Mail-Versand; Standort Deutschland.
- netcup GmbH, Emmy-Noether-Straße 10, 76131 Karlsruhe, Deutschland: Betrieb der Okto-Plattform; Rechenzentrum Nürnberg.
- DigitalOcean, LLC, 105 Edgeview Drive, Ste. 425, Broomfield, CO 80021, USA: Infrastruktur der Okto-Plattform; gewählte Region FRA1 (Frankfurt am Main).
- Anthropic: KI-Modelle der Claude-Familie für die Bearbeitung von Aufträgen; Sitz USA.
- OpenAI: GPT-Modelle für die Bearbeitung von Aufträgen; Sitz USA.
- Google: Gemini-Modelle für die Bearbeitung von Aufträgen; Sitz der Konzernmutter USA.
- Higgsfield: Erzeugung von Bildern und Videos; Sitz USA.

Welche dieser KI-Anbieter einen Auftrag bearbeiten, hängt von Funktion, Aufgabe und Verfügbarkeit ab. Die jeweils vertragsschließende Gesellschaft und ihre Anschrift teilt der Anbieter auf Anfrage an datenschutz@mein-angestellter.de mit.